Journal of Pure and Applied Algebra 4 (1974) 205–229. © North-Holland Publishing Company

ON THE GROUP OF AUTOMORPHISMS OF A FUNCTION FIELD OF GENUS AT LEAST TWO *

Balwant SINGH
School of Mathematics, Tata Institute of Fundamental Research, Colaba, Bombay 5, India

Communicated by F. Oort
Received 31 July 1973

0. Introduction

Let k be an algebraically closed field of characteristic p and let K be an algebraic function field of one variable over k of genus $g \geqslant 2$. Let $G = \mathrm{Aut}_k K$, the group of all automorphisms of K/k. It is known that G is a finite group. This was proved by Hurwitz [4] for the case $p = 0$, by Schmid [7] for $p \neq 0$ and also by Iwasawa and Tamagawa [5] for arbitrary p. Hurwitz also proved that for $p = 0$, $|G| \leqslant 84(g-1)$, and that this upper bound for the order of G is the best possible in the sense that there exists a function field of genus $g = 3$ whose group of automorphisms has order $84(g-1)$. Roquette [6] has recently shown that the inequality $|G| \leqslant 84(g-1)$ is valid also for $p > 2g+1$ and for $2g+1 > p > g+1$. He has further shown that for $p = 2g+1$ the inequality $|G| \leqslant 84(g-1)$ is valid except in the case of the hyperelliptic field $K = k(x,y)$ with $y^p - y = x^2$, $p \geqslant 5$, and that in this exceptional case $|G| = 8g(g+1)(2g+1)$ (and $p = 2g+1$). Our aim in this paper is to find an upper bound for $|G|$ for "small" p, i.e. for $p \leqslant 2g+1$, and to show that this upper bound is the best possible in the above sense. In fact, we show (in Theorem 3.1) that if $0 < p \leqslant 2g+1$, then

$$|G| \leqslant \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right)\left(\frac{4pg^2}{(p-1)^2}+1\right),$$

and that the equality holds if K is one of the following two fields:

(i) $K = k(x,y)$ with $y^p - y = x^{p+1}$, $p \geqslant 3$ (Theorem 3.3);

(ii) $K = k(x,y)$ with $y^p - y = x^2$, $p \geqslant 5$ (Roquette's above example).

Note that for $p = 2g+1$ our expression giving the upper bound equals $8g(g+1)(2g+1)$ which shows already that the equality holds if K is defined as in (ii).

* During the course of this work, the author received financial support from the Mathematisch Instituut, Amsterdam.

For a prime divisor $\mathfrak{p}$ of K, let $G(\mathfrak{p})$ denote the group of all automorphisms of K/k leaving $\mathfrak{p}$ fixed. In order to obtain an upper bound for $|G|$, we find it necessary first to get an upper bound for $|G(\mathfrak{p})|$. This is done in Theorem 2.1, and we show in Theorem 2.2 that this upper bound is also the best possible.

The author wishes to express his sincere thanks to Professor F. Oort for suggesting this problem and for helpful discussions.

1. Preliminaries

We fix the following notation: k is an algebraically closed field of characteristic p. By a function field we mean an algebraic function field of one variable over k. If K is a function field, we denote by g_K its genus and by P_K the set of its prime divisors. For $\mathfrak{p} \in P_K$, we write $G(\mathfrak{p})$ for the group of automorphisms σ of K/k for which $\sigma(\mathfrak{p}) = \mathfrak{p}$. If K/L is a finite extension of function fields, $\mathfrak{q} \in P_L$, $\mathfrak{p} \in P_K$ and $\mathfrak{p}$ lies over $\mathfrak{q}$, then we denote by $e_{\mathfrak{p}|\mathfrak{q}}$ the ramification index of $\mathfrak{p}$ over $\mathfrak{q}$. Let K be a function field and let $G = \mathrm{Aut}_k K$. We note that, since k is algebraically closed, we have, for $\mathfrak{p} \in P_K$, $G(\mathfrak{p})$ = the inertia group of $\mathfrak{p}$ in the extension K/K^G, and if $G(\mathfrak{p})$ is finite, then $|G(\mathfrak{p})| = e_{\mathfrak{p}|\mathfrak{q}}$, where $\mathfrak{q} = \mathfrak{p} \cap K^G$.

In the sequel, we shall make extensive use of

Hurwitz' Formula. *Let K/L be a finite separable extension of function fields and let $n = [K : L]$. Then*

$$2g_K - 2 = (2g_L - 2)n + \deg \mathfrak{D}_{K/L},$$

where $\mathfrak{D}_{K/L}$ is the different of the extension K/L.

For a proof, see, for instance, [3, p. 462].

If the extension K/L is Galois, then Hurwitz' Formula can be stated in another form, more convenient for our purposes:

Hurwitz' Formula. *Let K/L be a finite Galois extension of degree n of function fields. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \in P_L$ be all the prime divisors of L ramified in K/L. Let $\mathfrak{p}_i$ be a prime divisor of K dividing $\mathfrak{q}_i$, let $e_i = e_{\mathfrak{p}_i|\mathfrak{q}_i}$ and let d_i be the exponent to which $\mathfrak{p}_i$ appears in $\mathfrak{D}_{K/L}$, $1 \leqslant i \leqslant r$. Then*

$$(2g_K - 2)/n = 2g_L - 2 + d_1/e_1 + \ldots + d_r/e_r.$$

Proof. Let h_i be the number of prime divisors of K lying over $\mathfrak{q}_i$. Then $h_i e_i = n$ for every i, and $\deg \mathfrak{D}_{K/L} = \sum_{i=1}^{r} h_i d_i$. Therefore,

$$n^{-1} \deg \mathfrak{D}_{K/L} = d_1/e_1 + \ldots + d_r/e_r.$$

In the statement of the following lemma, we let p be the characteristic exponent of k.

Lemma 1.1. *Let K be a function field, $\mathfrak{p} \in P_K$ and G a finite subgroup of $\mathrm{Aut}_k K$ leaving $\mathfrak{p}$ fixed. Let*

$$G = G_0 \supset G_1 \supset \ldots \supset G_m \supsetneq G_{m+1} = 1$$

be the sequence of higher ramification groups of $\mathfrak{p}$ in the extension K/K^G. Let $|G| = qp^\alpha$ with $q, \alpha \in \mathbf{Z}^+$, $(q, p) = 1$, and let d be the exponent of $\mathfrak{p}$ in $\mathfrak{D}_{K/K^G}$. Then:

(i) *each G_i is a normal subgroup of G_0;*

(ii) *$|G_1| = p^\alpha$, G_0/G_1 is a cyclic group of order q and, for $i \geq 1$, G_i/G_{i+1} is a direct product of cyclic subgroups of order p;*

(iii) *$d = \sum_{i=0}^{m}(|G_i| - 1)$. In particular, $d \geq (qp^\alpha - 1) + (p^\alpha - 1)$.*

For a proof, see [8, ch. IV].

Lemma 1.2. *Let K be a function field of genus $g \geq 1$* and let $\mathfrak{p} \in P_K$. *Then $|G(\mathfrak{p})| < \infty$. Moreover, if $p \mid |G(\mathfrak{p})|$, then $|G(\mathfrak{p})| \leq 6(2g-1)$.*

For a proof, see [5].

Lemma 1.3. *Let $L = k(x)$ be a rational function field and let $K = k(x, y)$ be a cyclic extension of L of degree p $(p > 0)$ defined by $y^p - y = f \in L$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be all the prime divisors of L ramified in K/L. Let v_i be the discrete valuation of L corresponding to $\mathfrak{q}_i$, $1 \leq i \leq r$. Then:*

(1) *$v_i(f) < 0$ for every i, $1 \leq i \leq r$;*

(2) *we can modify the generator y of $K = L(y)$ so that*

(i) *f has no pole in L outside the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$, and*

(ii) *$(v_1(f), p) = 1$;*

(3) *if $(v_1(f), p) = 1$ and if $\mathfrak{p}_1$ is a prime divisor of K lying over $\mathfrak{q}_1$, then the exponent of $\mathfrak{p}_1$ in $\mathfrak{D}_{K/L}$ is $(-v_1(f) + 1)(p-1)$;*

(4) *if $(v_1(f), p) = 1$, then an automorphism σ of L/k extends to an automorphism of K/k if and only if there exist $h \in L$ and $c \in \mathbf{F}_p^*$ such that $h^p - h = \sigma(f) - cf$.*

Proof. (For a proof of parts (3), (2) and (3), see also, for example, [2].)

(1) It is enough to prove that $v_1(f) < 0$. If $v_1(f) \geq 0$, then $f(\mathfrak{q}_1)$ is a well-defined element of k and the p distinct values of y in the equation $y^p - y = f(\mathfrak{q}_1)$ define p distinct prime divisors of K lying over $\mathfrak{q}_1$. This contradicts the assumption that $\mathfrak{q}_1$ is ramified in K/L. Thus $v_1(f) < 0$.

(2) Note first that $r \geq 1$. For, by Hurwitz' Formula applied to K/L, we have $2g_K - 2 = -2p + \deg \mathfrak{D}_{K/L}$, which shows that $\deg \mathfrak{D}_{K/L} > 0$ and $r \geq 1$. Modifying the generator x of $L = k(x)$, we may assume that $\mathfrak{q}_1$ is the pole divisor of x in L. Let $\mathfrak{q} \in P_L - \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$, and let v be the discrete valuation of L corresponding to $\mathfrak{q}$. We claim that if $v(f) < 0$, then $p \mid v(f)$. For let $\mathfrak{p}$ be a prime divisor of K lying over $\mathfrak{q}$ and let $\bar{v}$ be the corresponding discrete valuation of K. Then, since $\mathfrak{q}$ is not ramified in K/L, we have $\bar{v} \mid L = v$. Therefore $\bar{v}(y^p - y) = v(f) < 0$ implies $\bar{v}(y) < 0$ implies $\bar{v}(y^p - y) = p\bar{v}(y)$,

which shows that $p \mid v(f)$. Let now $a_2, \ldots, a_r \in k$ be such that $\mathfrak{q}_i$ is the zero divisor of $x - a_i$ in L, $2 \leqslant i \leqslant r$. Then, in view of (1), we can write

$$f = f_1 \prod_{i=2}^{r} (x-a_i)^{-\alpha_i} \prod_{j=1}^{s} (x-b_j)^{-\beta_j},$$

with $f_1 \in k[x]$, $s \in \mathbf{Z}^+$, $\alpha_i, \beta_j \in \mathbf{N}$, $b_j \in k$, $b_j \neq a_i$ for every i, j, and $f_1(a_i) \neq 0 \neq f_1(b_j)$ for every i, j. For such an expression of f, let us write $\beta(f) = \Sigma_{j=1}^{s} \beta_j$. Assuming that $\beta(f) > 0$, we show that we can modify y in such a way that $\beta(f)$ is decreased. This is enough for proving (i).

So assume that $\beta(f) > 0$. We may assume that $b_1 = 0$. By our observation above, we can write $\beta_j = p\gamma_j$ with $\gamma_j \in \mathbf{N}$, $1 \leqslant j \leqslant s$. Let

$$f_2 = f_1 \prod_{i=2}^{r} (x-a_i)^{\alpha_i(p-1)},$$

$$a = f_2(0),$$

$$z = y - a^{1/p} \prod_{i=2}^{r} (x-a_i)^{-\alpha_i} \prod_{j=1}^{s} (x-b_j)^{-\gamma_j},$$

$$f_3 = z^p - z.$$

Then it is easy to see that $\beta(f_3) < \beta(f)$. This proves (i).

Now to prove (ii), assume that y has been chosen so that f has no pole in L outside the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$. Then, with the notation above, we have

$$f = f_1 \prod_{i=2}^{r} (x-a_i)^{-\alpha_i}.$$

Let $n = \deg f_1$. Then $v_1(f) = -n + \Sigma_{i=2}^{r} \alpha_i$. We now show that, if $p \mid v_1(f)$, then we can modify y to increase $v_1(f)$. This is enough since, by (1), we always have $v_1(f) < 0$. So let $v_1(f) = -mp$ with $m \in \mathbf{N}$. Then $n = mp + \Sigma_{i=2}^{r} \alpha_i$. Let

$$f_4 = f_1 \prod_{i=2}^{r} (x-a_i)^{\alpha_i(p-1)}.$$

Then $\deg f_4 = p(m + \Sigma\alpha_i) = pt$, say. Write $f_4 = bx^{pt} + f_5$, $b \in k^*$, $f_5 \in k[x]$ with $\deg f_5 < pt$. Letting

$$y' = y - b^{1/p} x^t \prod_{i=2}^{r} (x-a_i)^{-\alpha_i},$$

we find that $v_1(y'^p - y') > v_1(f)$.

(3) We assume, as in (2), that $\mathfrak{q}_1$ is the pole divisor of x in L. Let $\bar{v}_1$ be the discrete valuation of K corresponding to $\mathfrak{p}_1$. Since $\mathfrak{q}_1$ is ramified in K/L, we have $\bar{v}_1 | L = pv_1$. Therefore, $\bar{v}_1(f) = pv_1(f)$, and from the equation $y^p - y = f$, we get $\bar{v}_1(y) = v_1(f)$ since $v_1(f) < 0$, by (1). Let $m = \bar{v}_1(y) = v_1(f)$. Since $(m, p) = 1$, there

exist $s, t \in \mathbf{Z}$ such that $sm - tp = 1$. We may assume that $s > 0$. Let $\pi = x^t y^s$. Then $\bar{v}_1(\pi) = 1$ since $\bar{v}_1(x) = pv_1(x) = -p$. Thus π is a uniformising parameter for $\mathfrak{p}_1$. Let σ be the automorphism of K/k defined by $\sigma(x) = x$, $\sigma(y) = y + 1$. Then σ is a generator of the group $\mathrm{Gal}(K/L)$. By Lemma 1.1 (iii), it is now enough to prove that $\bar{v}_1(\sigma(\pi) - \pi) = -m + 1$. This can be easily checked, using the fact that $\bar{v}_1(y) < 0$ and $s > 0$.

(4) Let σ' be an extension of σ to K. We can write $\sigma'(y) = h_0 + h_1 y + \ldots + h_{p-1}y^{p-1}$ with $h_i \in L$. Then

$$\sigma(f) = \sigma'(y^p - y) = \sum_{i=0}^{p-1} h_i^p y^{ip} - \sum_{i=0}^{p-1} h_i y^i = \sum_{i=0}^{p-1} h_i^p (y+f)^i - \sum_{i=0}^{p-1} h_i y^i$$

$$= \sum_{i=0}^{p-1} h_i' y^i,$$

say, with $h_i' \in L$. Since $\sigma(f) \in L$, we have $h_i' = 0$ for $i \geqslant 1$. In particular, we have

$$0 = h_{p-1}' = h_{p-1}^p - h_{p-1}, \quad 0 = h_{p-2}' = -fh_{p-1}^p + h_{p-2}^p - h_{p-2}, \quad \text{if } p \geqslant 3.$$

From this we get $h_{p-1} \in \mathbf{F}_p$ and $h_{p-2}^p - h_{p-2} = fh_{p-1}$. If $h_{p-1} \neq 0$, then $v_1(fh_{p-1}) = v_1(f)$ is negative, by (1). It follows that $v_1(h_{p-2}) < 0$ and $v_1(f) = pv_1(h_{p-2})$. This contradicts the assumption that $(v_1(f), p) = 1$. Therefore, $h_{p-1} = 0$ and $h_{p-2}^p = h_{p-2}$. By decreasing induction on i, we can thus prove that $h_{p-1} = \ldots = h_2 = 0$ and $h_1^p = h_1$. Thus $\sigma(f) = h_0^p - h_0 + h_1 f$. Since $h_1^p = h_1$, we have $h_1 \in \mathbf{F}_p$. Since σ' is an automorphism, we have $h_1 \neq 0$. Now take $h = h_0$ and $c = h_1$.

Conversely, given h and c, we can extend σ to K by defining $\sigma'(y) = h + cy$.

2. An upper bound for $|G(\mathfrak{p})|$

Theorem 2.1. *Let k be an algebraically closed field of characteristic $p > 0$ and let K be a function field over k of genus $g \geqslant 1$. Let $G(\mathfrak{p})$ be the group of automorphisms of K/k leaving a prime divisor $\mathfrak{p}$ of K fixed. If p divides $|G(\mathfrak{p})|$, then*

$$|G(\mathfrak{p})| \leqslant \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right).$$

Proof. Let $G_0 = G(\mathfrak{p})$. By Lemma 1.2, $|G_0| < \infty$. Let $K_0 = K^{G_0}$ and let G_1 be the first ramification group of $\mathfrak{p}$ in the extension K/K_0. Let $|G_0| = qp^\alpha$ with $(q, p) = 1$, $\alpha \geqslant 1$. Then $|G_1| = p^\alpha$, by Lemma 1.1. Let $K_1 = K^{G_1}$ and $g_1 = g_{K_1}$. If $g_1 \geqslant 1$, then we have $q \leqslant 6(2g_1 - 1)$, by Lemma 1.2. For G_0/G_1 is a group of automorphisms of K_1/k of order q and leaves the prime divisor $\mathfrak{p}_1 = \mathfrak{p} \cap K_1$ of K_1 fixed. Also, by Hurwitz' Formula applied to K/K_1 and by Lemma 1.1, we have

$$\frac{2g-2}{p^\alpha} \geqslant 2g_1 - 2 + \frac{2p^\alpha - 2}{p^\alpha}$$

since $\mathfrak{p}$ is ramified in K/K_1 with ramification index p^α. This gives $g \geq g_1 p^\alpha$. Therefore,

$$|G_0| = qp^\alpha \leq 6(2g_1 p^\alpha - p^\alpha) \leq 6(2g-p) < \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right).$$

Assume therefore that $g_1 = 0$. We then have the following situation:

(i) K_1/K_0 is a Galois extension of degree q coprime to p and $g_{K_1} = 0$;

(ii) the ramification index of $\mathfrak{p}_1 = \mathfrak{p} \cap K_1$ in K_1/K_0 is q.

From this it can be checked by Hurwitz' Formula applied to K_1/K_0 (and by Lemma 1.1) that we have:

(iii) $g_{K_0} = 0$;

(iv) there exists a prime divisor, say $\mathfrak{q}_1$, of K_1, other than $\mathfrak{p}_1$, which has ramification index q in K_1/K_0;

(v) no prime divisor of K_1 other than $\mathfrak{p}_1, \mathfrak{q}_1$ is ramified in K_1/K_0.

Let p^β be the ramification index of $\mathfrak{q}_1$ in K/K_1, $0 \leq \beta \leq \alpha$. Let $G_0 \supset G_1 \supset \ldots \supset G_i \supsetneq G_{i+1} = \{1\}$ be the sequence of higher ramification groups of $\mathfrak{p}$ in the extension K/K_0. By Lemma 1.1, for $i \geq 1$, G_i/G_{i+1} is a direct product of cyclic groups of order p. We can therefore break up the extension K/K_1 into a tower of cyclic extensions of degree p. Let K' be the smallest field in this tower such that $g' = g_{K'} \geq 1$. Since $g \geq 1$, such a K' exists, and since $g_1 = 0$, we have $K' \supsetneq K_1$. Let K'' be the next smaller field in this tower, so that K'/K'' is a cyclic extension of degree p and $g_{K''} = 0$. Let s be the number of prime divisors of K'' ramified in K'/K''. Since $\mathfrak{p}'' = \mathfrak{p} \cap K''$ is ramified in K'/K'', we have $s \geq 1$. We now consider the two cases $s \geq 2$ and $s = 1$.

Case I: $s \geq 2$. Let $\mathfrak{r}'' \in P_{K''}$, $\mathfrak{r}'' \neq \mathfrak{p}''$, be such that $\mathfrak{r}''$ is ramified in K'/K'' and let $\mathfrak{r}_1 = \mathfrak{r}'' \cap K_1$. Let $\mathfrak{p}_0 = \mathfrak{p}_1 \cap K_0$, $\mathfrak{r}_0 = \mathfrak{r}_1 \cap K_0$ and $\mathfrak{q}_0 = \mathfrak{q}_1 \cap K_0$. Note that the ramification indices of $\mathfrak{p}_0, \mathfrak{q}_0$ in K/K_0 are qp^α, qp^β, respectively. Let us consider the two cases $\mathfrak{r}_1 \neq \mathfrak{q}_1$ and $\mathfrak{r}_1 = \mathfrak{q}_1$.

Case I(a): $\mathfrak{r}_1 \neq \mathfrak{q}_1$. In this case, by (v) above, the ramification index of $\mathfrak{r}_0$ in K/K_0 is a power of p, say p^γ, $\gamma \geq 1$. Therefore, by Hurwitz' Formula applied to K/K_0 and by Lemma 1.1, we have

$$\frac{2g-2}{qp^\alpha} \geq -2 + \frac{qp^\alpha - 1 + p^\alpha - 1}{qp^\alpha} + \frac{qp^\beta - 1 + p^\beta - 1}{qp^\beta} + \frac{2p^\gamma - 2}{p^\gamma}$$

$$= \frac{p^\alpha - 2}{qp^\alpha} + \frac{p^\beta - 2}{qp^\beta} + \frac{2p^\gamma - 2}{p^\gamma} \geq \frac{qp^\alpha - 2}{qp^\alpha}.$$

This gives

$$qp^\alpha \leq 2g < \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right).$$

Case I(b): $\mathfrak{r}_1 = \mathfrak{q}_1$. Let $[K : K'] = p^\delta$, $[K'' : K_1] = p^\epsilon$. Then $\delta + \epsilon + 1 = \alpha$. Since $g_{K''} = 0$ and $\mathfrak{p}_1$ is totally ramified in K''/K_1, it is easily seen by Hurwitz' Formula applied to K''/K_1 (and Lemma 1.1) that no prime divisor of K_1, other than $\mathfrak{p}_1$, is ramified in K''/K_1. Therefore, $\mathfrak{r}_1$ splits into p^ϵ prime divisors of K'', $\mathfrak{r}''$ among them.

Since $\mathfrak{r}''$ is ramified in K'/K'', all these p^e prime divisors are ramified in K'/K''. Now, since K'' is rational, there exists $x \in K''$ such that $K'' = k(x)$. We may choose x in such a way that $\mathfrak{p}'' = (x)_\infty$, $\mathfrak{r}'' = (x)_0$, i.e., $\mathfrak{p}''$, $\mathfrak{r}''$ are respectively the pole divisor and the zero divisor of x in K''. Since K'/K'' is a cyclic extension of degree p, it is an Artin–Schreier extension, i.e., there exists $y \in K'$ such that $K' = k(x, y)$ and $y^p - y = f \in K''$. Let us write $f = x^{-m} f_1$ with $m \in \mathbf{Z}$, $f_1 \in K''$, $f_1(0) \neq 0, \infty$. Then by Lemma 1.3, $m > 0$, and we may modify y and f to assume that $(m, p) = 1$. It then follows from the same lemma that the exponent in $\mathfrak{D}_{K'/K''}$ of a prime divisor $\mathfrak{r}'$ of K' lying over $\mathfrak{r}''$ is $(m+1)(p-1)$. Since the prime divisors of K' lying over the p^e prime divisors of K'' into which $\mathfrak{r}_1$ splits all lie over the same prime divisor $\mathfrak{r}_1$ of K_1, they all have the same exponent in $\mathfrak{D}_{K'/K''}$, which is $(m+1)(p-1)$. The exponent of $\mathfrak{p}' = \mathfrak{p} \cap K'$ in $\mathfrak{D}_{K'/K''}$ is, in any case, at least $2(p-1)$, by Lemma 1.1. Therefore, by Hurwitz' Formula applied to K'/K'', we have

$$\frac{2g'-2}{p} \geq -2 + \frac{2p-2}{p} + p^e \frac{(m+1)(p-1)}{p},$$

which gives

$$(*) \qquad 2g' \geq p^e(m+1)(p-1).$$

Since $\mathfrak{r}_1 = \mathfrak{q}_1$, $\mathfrak{r}_1$ is ramified in K_1/K_0 with ramification index q. Also, as we have observed, $\mathfrak{r}_1$ is not ramified in K''/K_1. Therefore, by Lemma 1.1, the inertia group $G(\mathfrak{r}'')$ of $\mathfrak{r}''$ in the extension K''/K_0 is cyclic of order q. Let $\sigma \in G(\mathfrak{r}'') \subset \mathrm{Gal}(K''/K_0)$ be a generator of $G(\mathfrak{r}'')$. Since K'' is rational with x as a generator, we have $\sigma(x) = (ax+b)/(cx+d)$ with $a, b, c, d \in k$, $ad - bc \neq 0$. Since σ fixes the prime divisors $\mathfrak{p}'' = (x)_\infty$ and $\mathfrak{r}'' = (x)_0$ of K'', we have, in fact, $\sigma(x) = ax$ with $a \in k^*$. Since the order of σ is q, a is a primitive q^{th} root of unity. Now since $\mathrm{Gal}(K''/K_0)$ is a quotient of $\mathrm{Gal}(K'/K_0)$, σ extends to an automorphism of K'/k. Therefore, by Lemma 1.3, there exist $h \in K''$ and $c \in \mathbf{F}_p^*$ such that

$$h^p - h = f(ax) - cf = a^{-m} x^{-m} f_1(ax) - c\, x^{-m} f_1.$$

Write $h = x^n h_1$ with $n \in \mathbf{Z}$, $h_1 \in K''$, $h_1(0) \neq 0, \infty$. Then

$$x^{np}(h_1^p - x^{-n(p-1)} h_1) = a^{-m} x^{-m} (f_1(ax) - a^m c f_1).$$

Since $m > 0$ and $(m, p) = 1$, it follows that $f_1(0) - a^m c f_1(0) = 0$. Since $f_1(0) \neq 0$, this implies that $a^m c = 1$ implies $a^m \in \mathbf{F}_p^*$ implies $a^{m(p-1)} = 1$ implies $q \leq m(p-1)$. Therefore, by (*), we have

$$(**) \qquad qp^e \leq p^e m(p-1) < 2g'.$$

Now, by Hurwitz' Formula applied to K/K' and by Lemma 1.1, we have

$$\frac{2g-2}{p^\delta} \geq 2g' - 2 + \frac{2p^\delta - 2}{p^\delta}$$

since $\mathfrak{p}' = \mathfrak{p} \cap K'$ is ramified in K/K' with ramification index p^δ. This gives $g \geq g' p^\delta$.

Therefore,

$$|G_0| = q\,p^{\epsilon}\,p\,p^{\delta} < 2g'\,p\,p^{\delta} \qquad \text{(by (**))}$$
$$\leqslant 2p\,g.$$

To show now that $2pg \leqslant (4pg^2/(p-1))\,(2g/(p-1)+1)$, we first apply Hurwitz' Formula to K/K_1 to get

$$\frac{2g-2}{p^{\alpha}} \geqslant -2 + \frac{2p^{\alpha}-2}{p^{\alpha}} + \frac{2p^{\beta}-2}{p^{\beta}}, \qquad \beta \geqslant 1,$$

since, by assumption, $\mathfrak{r}_1 = \mathfrak{q}_1$ is ramified in K/K_1 with ramification index p^{β}. This gives

$$\frac{2g}{p^{\alpha}} \geqslant \frac{2p^{\beta}-2}{p^{\beta}} \geqslant \frac{2p-2}{p},$$

so that

$$p^{\alpha} \leqslant pg/(p-1) \quad \text{and} \quad p-1 \leqslant g.$$

Therefore $g/(p-1) \geqslant 1$, and we get

$$\frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right) \geqslant 12pg > 2pg \geqslant |G_0|.$$

Case II: $s = 1$. In this case, $\mathfrak{p}''$ is the only prime divisor of K'' ramified in K'/K''. Choose $x \in K''$ such that $K'' = k(x)$ and $\mathfrak{p}''$ is the pole divisor of x in K''. There exists $y \in K'$ such that $K' = k(x, y)$ and $y^p - y = f \in K''$. By Lemma 1.3, we may assume that $\mathfrak{p}''$ is the only pole of f in K'', i.e., $f \in k[x]$. Let $m = \deg f$. By Lemma 1.3, we may assume that $(m, p) = 1$. It then follows from the same lemma that the exponent of $\mathfrak{p}' = \mathfrak{P} \cap K'$ in $\mathfrak{D}_{K'/K''}$ is $(m+1)(p-1)$. Since $\mathfrak{p}''$ is the only prime divisor of K'' ramified in K'/K'' and it is totally ramified, we get $\deg \mathfrak{D}_{K'/K''} = (m+1)(p-1)$. Therefore, we see by Hurwitz' Formula applied to K'/K'' that

$$2g' = (m-1)(p-1).$$

Note that $g' \geqslant 1$ implies $m \geqslant 2$. Let $f = f_m x^m + \ldots + f_0$, $f_i \in k$, $f_m \neq 0$. Let $H = \mathrm{Gal}(K''/K_0)$. Since K'' is rational with x as a generator, every $\sigma \in H$ can be represented in the form $\sigma(x) = (ax+b)/(cx+d)$ with $a, b, c, d \in k$ and $ad - bc \neq 0$. Since $\sigma \in H$ implies $\sigma(\mathfrak{p}'') = \mathfrak{p}''$, and $\mathfrak{p}'' = (x)_{\infty}$, we can in fact represent σ in the form $\sigma(x) = ax + b$ with $a, b \in k$, $a \neq 0$. This gives an injective mapping

$$\rho : H \to k^* \times k: \qquad \sigma \mapsto (a, b).$$

Claim. *For every $c \in \mathbf{F}_p^*$ and for every $a \in k^*$ with $a^m = c$, there exists a non-zero polynomial $F_{a,c}(T)$ in T with coefficients in $\mathbf{F}_p(f_0, \ldots, f_m, a, c)$ and of degree $\leqslant (m-1)^2$ such that*

$$\mathrm{im}\,\rho \subset \bigcup_{c \in \mathbf{F}_p^*} \bigcup_{\substack{a \in k^* \\ a^m = c}} \{(a, b): F_{a,c}(b) = 0\}.$$

Assume the claim for a moment. Then

$$|H| = |\operatorname{im}\rho| \leqslant (p-1)\,m\,(m-1)^2 = \frac{4g'^2}{p-1}\left(\frac{2g'}{p-1}+1\right)$$

since $2g' = (m-1)(p-1)$. If $[K:K'] = p^\delta$, then as in Case 1(b), we have $g' \leqslant g'\,p^\delta \leqslant g$. Therefore we get

$$|G_0| = |H|\,p^{\delta+1} \leqslant \frac{4p\,p^\delta\,g'^2}{p-1}\left(\frac{2g'}{p-1}+1\right) \leqslant \frac{4p\,g^2}{p-1}\left(\frac{2g}{p-1}+1\right).$$

Proof of the Claim. Let $\sigma \in H$ and $\sigma(x) = ax + b$ so that $\rho(\sigma) = (a, b)$. Since $H = \mathrm{Gal}(K''/K_0)$ is a quotient of $\mathrm{Gal}(K'/K_0)$, there exists $\sigma' \in \mathrm{Gal}(K'/K_0)$ such that $\sigma' \mid K'' = \sigma$. Therefore, by Lemma 1.3, there exist $h \in K''$ and $c \in \mathbf{F}_p^*$ such that

$$h^p - h = \sigma(f) - cf = f(ax+b) - cf.$$

Thus $h^p - h \in k[x]$ which implies that $h \in k[x]$. Write $m = tp + u$, $t, u \in \mathbf{Z}^+$, $1 \leqslant u \leqslant p-1$. (Recall that $(m, p) = 1$.) Then $\deg(h^p - h) \leqslant m = tp + u$ implies that $\deg h \leqslant t$. Therefore we can write

$$h = h_t\,x^t + \ldots + h_1 x + h_0, \qquad h_i \in k$$

(h_t may be zero). Now $\deg(h^p - h) \leqslant tp \leqslant m-1$. Therefore, comparing the coefficients of x^m in the identity

$$h^p - h = f(ax+b) - cf,$$

we get $0 = f_m(a^m - c)$, which implies $a^m = c$. In order now to define the polynomial $F_{a,c}(T)$, we consider the two cases $t = 0$ and $t \neq 0$.

Case 1: $t = 0$. In this case, $\deg(h^p - h) \leqslant 0$. Therefore, comparing the coefficients of x in

$$h^p - h = f(ax+b) - cf,$$

we get

$$0 = m\,f_m\,ab^{m-1} + (m-1)f_{m-1}\,a\,b^{m-2} + \ldots + 2f_2\,a\,b + f_1\,a - c\,f_1.$$

Thus $F_{a,c}(T) = m\,f_m\,a\,T^{m-1} + \ldots + f_1\,a - c\,f_1$ is the required polynomial in this case. Note that since $(m, p) = 1$, $f_m \neq 0$ and $a \neq 0$, $F_{a,c}(T)$ is a non-zero polynomial of degree $= m-1$.

Case 2: $t \geqslant 1$. We write $t = sp^r$ with $s, r \in \mathbf{Z}^+$, $(s, p) = 1$. For $0 \leqslant i \leqslant r+1$, let $F_i(b)$ be the coefficient of x^{sp^i} in $f(ax+b) - cf$. Then putting $j = sp^i$, we have

$$F_i(b) = \binom{m}{j} f_m\,a^j\,b^{m-j} + \binom{m-1}{j} f_{m-1}\,a^j\,b^{m-1-j} + \ldots + f_j\,a^j - f_j\,c,$$

so that $F_i(b)$ is a polynomial in b with coefficients in $\mathbf{F}_p(f_0, \ldots, f_m, a, c)$ and of degree $\leqslant m-j = m-sp^i$. Let us now compare the coefficients of x^{sp^i} in $h^p - h = f(ax+b) - cf$, $0 \leqslant i \leqslant r+1$; see Table 1.

Table 1

Coefficient of	in $h^p - h$		in $f(ax+b) - cf$
$x^{sp^{r+1}}$	$h^p_{sp^r}$	=	$F_{r+1}(b)$
x^{sp^r}	$h^p_{sp^{r-1}} - h_{sp^r}$	=	$F_r(b)$
⋮	⋮		⋮
x^{sp^i}	$h^p_{sp^{i-1}} - h_{sp^i}$	=	$F_i(b)$
⋮	⋮		⋮
x^{sp}	$h^p_s - h_{sp}$	=	$F_1(b)$
x^s	$-h_s$	=	$F_0(b)$

From this we get

$$(*) \qquad ((\ldots((-F_0)^p - F_1)^p - \ldots)^p - F_r)^p = F_{r+1},$$

where $F_i = F_i(b)$. Since F_i is a polynomial in b of degree $\leqslant m - sp^i$, it follows that the left-hand side is a polynomial in b of degree

$$\leqslant mp^{r+1} - sp^{r+1} = (m-s)\,p^{r+1} \leqslant (m-1)^2$$

since $m = sp^{r+1} + u \geqslant p^{r+1} + 1$. It is also easy to see that the right-hand side is a non-zero polynomial in b of degree $u < m-1$. Moreover, since the left-hand side is a polynomial in b^p and the right-hand side is not (u being coprime to p), the relation $(*)$ does not hold identically for all b. Thus

$$F_{a,c}(T) = ((\ldots((-F_0(T))^p - F_1(T))^p - \ldots)^p - F_r(T))^p - F_{r+1}(T)$$

is a non-zero polynomial in T of degree $\leqslant (m-1)^2$, and our claim is proved.

This completes the proof of Theorem 2.1.

Theorem 2.2. (i) *Let $p > 0$ and let $K = k(x, y)$ with $y^p - y = f$, where $f \in k[x]$ is a polynomial of degree $p^r + 1$, $r \in \mathbf{Z}^+$. Assume that $r \geqslant 1$ if $p = 2$. Let $\mathfrak{p}$ be a prime divisor of K lying over the pole divisor of x in $k(x)$ and let $g = g_K$. Then:*

(1) *$2g = p^r(p-1)$ and, in particular, $g \geqslant 1$;*

(2) *$\mathfrak{p}$ is the only prime divisor of K lying over the pole divisor of x in $k(x)$;*

(3) *$G(\mathfrak{p}) \supset \{\sigma \in \mathrm{Aut}_k K\colon \sigma(x) \in k(x)\}$.*

(ii) *With the notation of* (i), *assume further that $f = x^{p^{r+1}}$. Then we have*

$$|G(\mathfrak{p})| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right).$$

(iii) *Conversely, let $p > 0$ and let K/k be a function field of genus $g \geqslant 1$. If there exists a prime divisor $\mathfrak{p}$ of K such that*

$$|G(\mathfrak{p})| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right),$$

then there exist $x, y \in K$ *and* $r \in \mathbf{Z}^+$ *such that*

(1) $2g = p^r(p-1)$;

(2) K *is defined by* $K = k(x, y)$ *with* $y^p - y = f$, *where* $f \in k[x]$ *is a polynomial of degree* p^r+1;

(3) $\mathfrak{p}$ *is the unique prime divisor of* K *lying over the pole divisor of* x *in* $k(x)$ *and we have*

$$G(\mathfrak{p}) \supset \{\sigma \in \mathrm{Aut}_k K: \sigma(x) \in k(x)\}.$$

Proof. (i) Let $K = k(x, y)$ with $y^p - y = f \in k[x]$ and $\deg f = p^r + 1$. Let $K' = k(x)$ and let $\mathfrak{p}'$ be the pole divisor of x in K'. We see by Hurwitz' Formula applied to K/K' that some prime divisor of K' is ramified in K/K' and it follows from Lemma 1.3 that $\mathfrak{p}'$ is the only prime divisor of K' ramified in K/K' (since $f \in k[x]$). Since $[K : K'] = p$, $\mathfrak{p}'$ is totally ramified in K/K' and it follows that $\mathfrak{p}$ is the only prime divisor of K lying over $\mathfrak{p}'$ and it is also the only prime divisor of K ramified in K/K'. Therefore, the degree of $\mathfrak{D}_{K/K'}$ equals the exponent of $\mathfrak{p}$ in $\mathfrak{D}_{K/K'}$, which is equal to $(p^r+2)(p-1)$ by Lemma 1.3. (Note that our assumption $r \geqslant 1$ if $p = 2$ ensures that $(p^r+1, p) = 1$.) It therefore follows from Hurwitz' Formula applied to K/K' that $2g = p^r(p-1)$. Finally, since $\mathfrak{p}$ is the only prime divisor of K ramified in K/K', every automorphism of K/k which carries K' into K' belongs to $G(\mathfrak{p})$. This completes the proof of (i).

(ii) Since $g \geqslant 1$, we have $|G(\mathfrak{p})| < \infty$, by Lemma 1.2. Let

$$H = \{\sigma \in \mathrm{Aut}_k K: \sigma(K') \subset K'\}.$$

Then, by (i), $H \subset G(\mathfrak{p})$ and therefore $|H| < \infty$.

Claim. $p \mid |H|$ *and* $|H| \geqslant p^{2r+1}(p-1)(p^r+1)$.

Assume the claim for a moment. Then, since $H \subset G(\mathfrak{p})$, we get $p \mid |G(\mathfrak{p})|$ and therefore

$$\begin{aligned} \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right) &\geqslant |G(\mathfrak{p})| \qquad \text{(by Theorem 1)} \\ &\geqslant |H| \\ &\geqslant p^{2r+1}(p-1)(p^r+1) \\ &= \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right). \end{aligned}$$

To prove the claim, let $\varphi: H \to \mathrm{Aut}_k K'$ be the restriction homomorphism. Since $[K : K'] = p$, we have $|\ker \varphi| = p$ and $|H| = p\,|\mathrm{im}\,\varphi|$. Therefore, it is enough to prove that $|\mathrm{im}\,\varphi| \geqslant p^{2r}(p-1)(p^r+1)$. Let

$$H' = \{\sigma \in \mathrm{Aut}_k K': \sigma(x) = ax + b \text{ with } a, b \in k,\ a^{(p^r+1)(p-1)} = 1 \text{ and } b^{p^{2r}} + b = 0\}.$$

Then, clearly, $|H'| = p^{2r}(p-1)(p^r+1)$, and it suffices to show that $H' \subset \operatorname{im}\varphi$. In other words, we have to show that any element of H' extends to an automorphism of K/k. So let $\sigma \in H'$, $\sigma(x) = ax + b$ with $a, b \in k$ satisfying

$$(*) \qquad a^{(p^r+1)(p-1)} = 1, \qquad b^{p^{2r}} + b = 0.$$

To show that σ extends to an automorphism of K/k, it is enough, by Lemma 1.3, to show that there exist $c \in \mathbf{F}_p^*$ and $h \in K'$ such that

$$h^p - h = (ax + b)^{p^r+1} - c\,x^{p^r+1}.$$

Let us define

$$c = a^{p^r+1}, \qquad h = h_0 + \sum_{i=1}^{r} h_i\, x^{p^{i-1}},$$

where $h_i \in k$ are defined as

$$h_1 = -a\,b^{p^r}, \qquad h_{i+1} = h_i^p, \quad 1 \leqslant i \leqslant r-1,$$

and h_0 is any element of k satisfying

$$h_0^p - h_0 = b^{p^r+1}.$$

It is then easily checked, using conditions (*), that c and h so defined satisfy the requirement. This completes the proof of (ii).

(iii) Parts (1) and (2) follow directly from the proof of Theorem 2.1. For, except in Case II in that theorem, we have obtained the strict inequality

$$|G(\mathfrak{p})| < \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right).$$

On the other hand, in Case II the equality

$$|G(\mathfrak{p})| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)$$

occurs only if, with the notation as in Theorem 2.1, we have $\delta = 0$ and $\deg F_{a,c}(T) = (m-1)^2$ for every a, c. Also $\deg F_{a,c}(T) = (m-1)^2$ only if $m = p^r + 1$ for some $r \in \mathbf{Z}^+$. This proves (1) and (2). Part (3) now follows from (i), noting that, as in Case II of Theorem 2.1, we can choose $x, y \in K$ such that $\mathfrak{p}$ lies over the pole divisor of x in $k(x)$.

Remark 2.3. The proof of Theorem 2.1 giving an upper bound for $|G(\mathfrak{p})|$ could have been shortened a bit. However, in the course of that proof, we have obtained in some cases upper bounds for $|G(\mathfrak{p})|$ which are sharper than the one mentioned in the statement of the theorem. We shall require these sharper bounds for the proof of Theorem 3.1. In the following lemma, we summarise some of the results which have been obtained in the course of the proof of Theorem 2.1, but not mentioned in its statement.

Lemma 2.4. *Let the notation and assumption be as in Theorem 2.1. Let* $|G(\mathfrak{p})| = qp^{\alpha}$, $(q, p) = 1, \alpha \geqslant 1$. *Then:*

(i) *either* $p = 2g + 1$ *or* $p \leqslant g + 1$;

(ii) $q \leqslant 6g-2$ *and* $p^{\alpha} \leqslant 4pg^2/(p-1)^2$;

(iii) *if Case* II *occurs, then* $q \leqslant 2g' + p - 1$.

Proof. If $g_1 \geqslant 1$, then $g \geqslant g_1 p^{\alpha} \geqslant p^{\alpha} \geqslant p$. Therefore, we also have $4pg^2/(p-1)^2 > 4g > p^{\alpha}$ and $q \leqslant 6(2g_1 - 1) < 6g-2$. This proves both (i) and (ii) in this case.

So assume that $g_1 = 0$ and look at the cases considered in Theorem 2.1.

Case I(a). In this case, we have $qp^{\alpha} \leqslant 2g$ which implies $q \leqslant g < 6g-2$. Moreover, by Hurwitz' Formula applied to K/K_1, we get

$$\frac{2g-2}{p^{\alpha}} \geqslant -2 + \frac{2p^{\alpha}-2}{p^{\alpha}} + \frac{2p^{\gamma}-2}{p^{\gamma}}$$

which gives $p^{\alpha} \leqslant pg/(p-1)$, since $\gamma \geqslant 1$. This also shows that $p-1 \leqslant g$ and $pg/(p-1) < 4pg^2/(p-1)^2$.

Case I(b). In this case, we have proved $qp^{\alpha} \leqslant 2pg$, $p^{\alpha} \leqslant pg/(p-1)$ and $p-1 \leqslant g$. This proves both (i) and (ii) in this case.

Case II. In this case, we have $g \geqslant g'p^{\delta}$ and $2g' = (m-1)(p-1)$ with $m \geqslant 2$. If $\delta > 0$, then $g \geqslant 2g' \geqslant p-1$. If $\delta = 0$, then $2g = (m-1)(p-1)$ and it follows that $2g = p-1$ or $g \geqslant p-1$. This proves (i). Now choose $\sigma \in H = \mathrm{Gal}(K''/K_0)$ such that $\sigma | K_1$ is a generator of G_0/G_1. (Note that G_0/G_1 is a quotient of H and is cyclic of order q, by Lemma 1.1.) Let $\sigma(x) = ax + b$. Then a is a primitive q^{th} root of unity. Now, by the "Claim" in Case II of Theorem 2.1, $a^{m(p-1)} = 1$. Therefore,

$$q \leqslant m(p-1) = 2g' + p - 1 \leqslant 4g'.$$

This proves (iii) and also that $q \leqslant 4g \leqslant 6g - 2$. Finally, let $H_1 = \mathrm{Gal}(K''/K_1)$. Then H_1 is a subgroup of H. If $\sigma \in H_1$ and $\sigma(x) = ax + b$, then $a = 1$ since the order of σ is a power of p. Therefore $c = a^m = 1$, and the "Claim" of Theorem 2.1, Case II, implies that

$$\rho(H_1) \subset \{(1, b): F_{1,1}(b) = 0\}.$$

Thus

$$|H_1| = |\rho(H_1)| \leqslant (m-1)^2 = 4g'^2/(p-1)^2.$$

Therefore

$$p^{\alpha} = |G_1| = p^{\delta+1}\,|H_1| \leqslant 4pp^{\delta}g'^2/(p-1)^2 \leqslant 4pg^2/(p-1)^2$$

since $p^{\delta}g' \leqslant g$. This proves (ii), and the lemma is completely proved.

3. An upper bound for $|G|$

Theorem 3.1. *Let* K *be a function field of genus* $g \geqslant 2$ *over an algebraically closed field* k *of characteristic* p. *Let* $G = \mathrm{Aut}_k K$. *Then:*

(1) *If* $p \nmid |G(\mathfrak{p})|$ *for every* $\mathfrak{p} \in P_K$, *then* $|G| \leqslant 84(g-1)$.
(2) *If there exists* $\mathfrak{p} \in P_K$ *such that* $p \mid |G(\mathfrak{p})|$, *then*

$$|G| \leqslant \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right)\left(\frac{4pg^2}{(p-1)^2}+1\right)$$

and the equality holds if $K = k(x, y)$ *with*
(i) $y^p - y = x^{p+1}$, $p \geqslant 3$, *or*
(ii) $y^p - y = x^2$, $p \geqslant 5$.

Remark 3.2. If there exists $\mathfrak{p} \in P_K$ such that $p \mid |G(\mathfrak{p})|$, then $p \leqslant 2g+1$, by Lemma 2.4. Therefore, if $p > 2g+1$, then the inequality in (1) is valid. Moreover, if $0 < p \leqslant 2g+1$, then

$$84(g-1) < \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right)\left(\frac{4pg^2}{(p-1)^2}+1\right),$$

as can be checked easily. Therefore, if $0 < p \leqslant 2g+1$, then the inequality

$$|G| \leqslant \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right)\left(\frac{4pg^2}{(p-1)^2}+1\right)$$

holds in any case.

Proof of Theorem 3.1. With the notation of Hurwitz' Formula, we have

$$(2g-2)/n = 2g_L - 2 + d_1/e_1 + \ldots + d_r/e_r,$$

where $n = |G|$ and $L = K^G$. By Lemma 1.1, we have $d_i \geqslant e_i - 1$ for every i, $1 \leqslant i \leqslant r$. With this in mind, a glance at Hurwitz' proof in [4] of the inequality $|G| \leqslant 84(g-1)$ for $p = 0$ shows that this inequality continues to be valid if any of the following four conditions is satisfied:

(a) $g_L \geqslant 1$;
(b) $r \geqslant 5$;
(c) $r = 4$ and at least one of e_1, e_2, e_3, e_4 is different from 2;
(d) $r = 3$ and, assuming $e_1 \geqslant e_2 \geqslant e_3$, the triple (e_1, e_2, e_3) does not take one of the values listed in Table 2.

Moreover, if $p \nmid e_i$ for every i, then $d_i = e_i - 1$ for every i, $1 \leqslant i \leqslant r$ (Lemma 1.1), and one of the above four conditions is necessarily satisfied (since $g \geqslant 2$). On the other hand, if $p \mid e_i$ for some i, then by Lemma 2.4 we have $p \leqslant 2g+1$, so that

$$\frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right)\left(\frac{4pg^2}{(p-1)^2}+1\right) > 84(g-1),$$

as we have remarked above. Therefore, we need only prove:

(A) *the inequality in* (2) *under the assumption that none of the above four conditions* (a)–(d) *is satisfied*;

(B) *the statement about the equality in* (2).

Table 2

e_1	e_2	e_3
3	3	3
4	4	2
6	3	2
5	3	2
4	3	2
3	3	2
e_1 (arbitrary)	2	2

We shall prove (B) in Theorem 3.3. We now proceed to prove (A). Since we have assumed that none of the conditions (a)–(d) is satisfied, we have $g_L = 0$ and one of the following four cases occurs:

Case I: $r = 4$ and $e_1 = e_2 = e_3 = e_4 = 2$.

Case II: $r = 3$ and, assuming $e_1 \geqslant e_2 \geqslant e_3$, the triple (e_1, e_2, e_3) takes one of the values mentioned in Table 2.

Case III: $r = 1$.

Case IV: $r = 2$.

(Note that, since $g \geqslant 2$, we cannot have $g_L = 0$ and $r = 0$.) We discuss these four cases separately. As will be seen, the only non-trivial case is IV. Let us write

$$B(p, g) = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)\left(\frac{4pg^2}{(p-1)^2} + 1\right).$$

Case I. We have

$$(2g-2)/n = -2 + \tfrac{1}{2}d_1 + \tfrac{1}{2}d_2 + \tfrac{1}{2}d_3 + \tfrac{1}{2}d_4 = \tfrac{1}{2}d \quad \text{with some } d \in \mathbf{Z}.$$

Since $g \geqslant 2$, we have $d > 0$. Therefore $(2g-2)/n \geqslant \frac{1}{2}$ and $n \leqslant 4(g-1) < B(p, g)$.

Case II. We have

$$(2g-2)/n = -2 + d_1/e_1 + d_2/e_2 + d_3/e_3 \geqslant 1/\mathrm{lcm}(e_1, e_2, e_3)$$

since $g \geqslant 2$ implies that the right-hand side is positive. Now, if (e_1, e_2, e_3) takes one of the first six values mentioned in Table 2, then $\mathrm{lcm}(e_1, e_2, e_3) \leqslant 30$. Therefore $n \leqslant 60(g-1) < B(p, g)$ since $p \leqslant 2g + 1$, by Lemma 2.4. Now suppose that e_1 is arbitrary and $e_2 = e_3 = 2$. Then

$$(2g-2)/n = -2 + d_1/e_1 + \tfrac{1}{2}d_2 + \tfrac{1}{2}d_3.$$

If $p = 2$, then $d_2 \geqslant 2, d_3 \geqslant 2$, by Lemma 1.1, so that

$$(2g-2)/n \geqslant d_1/e_1 \geqslant \tfrac{1}{2}$$

since $d_1 \geq e_1 - 1$. This gives $n \leq 4(g-1) < B(p, g)$. If $p \neq 2$, then $p \mid e_1$. For, by assumption, p divides at least one of e_1, e_2, e_3. Let $e_1 = qp^\alpha$ with $(q, p) = 1, \alpha \geq 1$. Then, by Lemma 1.1, $d_1 \geq qp^\alpha - 1 + p^\alpha - 1$. Therefore,

$$\frac{2g-2}{n} \geq -2 + \frac{qp^\alpha + p^\alpha - 2}{qp^\alpha} + \tfrac{1}{2} + \tfrac{1}{2} = \frac{p^\alpha - 2}{qp^\alpha} \geq \frac{1}{3q}$$

since $p \geq 3$. Therefore $n \leq 6q(g-1) \leq 6(6g-2)(g-1)$, by Lemma 2.4. Also, $6(6g-2)(g-1) < B(p, g)$ since $p \leq 2g+1$, by Lemma 2.4.

Case III: $r = 1$. In this case, we have

$$(2g-2)/n = -2 + d_1/e_1 \geq 1/e_1$$

since $g \geq 2$. This gives $n \leq 2(g-1)e_1$. Now, by assumption, $p \mid e_1$. Therefore

$$e_1 \leq \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right),$$

by Theorem 2.1. Also, $2(g-1) < 4pg^2/(p-1)^2 + 1$ since $p \leq 2g+1$, by Lemma 2.4. Thus $n < B(p, g)$.

Case IV: $r = 2$. We have

$$(2g-2)/n = -2 + d_1/e_1 + d_2/e_2.$$

Let $d_i' = d_i - (e_i - 1), i = 1, 2$. Then

$$(2g-2)/n = (d_1' - 1)/e_1 + (d_2' - 1)/e_2.$$

Now $p \mid e_1$ or $p \mid e_2$, and we may assume that $p \mid e_1$. Let $e_1 = qp^\alpha$ with $(q, p) = 1$, $\alpha \geq 1$. Then, by Lemma 1.1, $d_1' \geq p^\alpha - 1$. If $p \mid e_2$ also, then $d_2' \geq 1$ and

$$\begin{aligned}(2g-2)/n &\geq (d_1' - 1)/e_1 \\ &= (p^\alpha - 2 + d'')/qp^\alpha, \quad \text{where } d'' = d_1' - (p^\alpha - 1) \geq 0, \\ &\geq 1/3q \qquad (\text{unless } d_1' = 1).\end{aligned}$$

This implies that $n \leq 6q(g-1) \leq 6(6g-2)(g-1)$, by Lemma 2.4. Since $p \leq 2g+1$, we have $6(6g-2)(g-1) < B(p, g)$. (If $d_1' = 1$, then, since $g \geq 2$, we have $d_2' \geq 2$ and we can apply the same argument with e_1 replaced by e_2.)

Now we consider the case when $p \nmid e_2$. Then $d_2' = 0$, by Lemma 1.2. Therefore,

$$(2g-2)/n = (d_1' - 1)/e_1 - 1/e_2 \geq 1/e_1 e_2$$

since $g \geq 2$ implies that the right-hand side is positive. This gives $n \leq 2e_1 e_2(g-1)$. Now, by Lemma 1.2, $(e_2, p) = 1$ implies that $e_2 \leq 6(2g-1)$. Therefore we get

$$(*) \qquad n \leq 12e_1(g-1)(2g-1).$$

Choose $\mathfrak{p} \in P_K$ such that e_1 is the ramification index of $\mathfrak{p}$ in K/L. We now adopt the same notation as in the proof of Theorem 2.1. Thus we let $G_0 = G(\mathfrak{p})$, $K_0 = K^{G_0}$,

G_1 = the first ramification group of $\mathfrak{p}$ in K/K_0. Then $|G_0| = qp^\alpha$ and $|G_1| = p^\alpha$. Let $g_1 = g_{K_1}$. We consider the two cases $g_1 \geq 1$ and $g_1 = 0$.

Case IV(a): $g_1 \geq 1$. Then, as in Theorem 2.1, we have

(i) $g_1 p^\alpha \leq g$;

(ii) $e_1 \leq 6(2g-p)$.

Therefore, from (*), we get

$$(**) \qquad n \leq 72\,(2g-p)\,(g-1)\,(2g-1).$$

Now, if $p = 2$, then

$$B(p, g) = 8g^2\,(2g+1)\,(8g^2+1) > 72\,(2g-p)\,(g-1)\,(2g-1) \geq n.$$

So assume that $p \geq 3$. Then, if $\alpha \geq 2$ or $g_1 \geq 3$, (i) implies $3p \leq g$. Therefore $2g/(p-1) > 6$, and we get

$$B(p, g) > 72\,(2g-p)\,(g-1)\,(2g-1) \geq n.$$

So let $\alpha = 1$ and $g_1 = 1$ or 2. By Hurwitz' Formula applied to K/K_1, we have

$$2g - 2 = (2g_1 - 2)p + \deg \mathfrak{D}_{K/K_1}.$$

By Lemma 1.1, we can write $\deg \mathfrak{D}_{K/K_1} = (\mu+2)(p-1)$ with $\mu \in \mathbf{Z}^+$. Therefore we get

$$2g = 2g_1 p + \mu(p-1).$$

This gives

$$\begin{aligned} n &\leq 72(2g-p)(g-1)(2g-1) \qquad \text{(by (**))} \\ &= 36\,(2g_1 p + \mu p - \mu - p)\,(2g_1 p + \mu p - \mu - 2)\,(2g_1 p + \mu p - \mu - 1) \\ &< B(p, \tfrac{1}{2}(2g_1 p + \mu p - \mu)) \qquad \text{if } \mu \geq 1. \end{aligned}$$

This last inequality can be easily checked, keeping in mind that $g_1 = 1$ or 2. We are thus reduced to considering the case $\mu = 0$. In this case, $g = g_1 p$. Let $u = [K_0 : L]$ so that $n = uqp$. If $u \leq (5g_1 + 1)qp$, then

$$n \leq (5g_1 + 1)\,q^2 p^2 \leq 36p^2\,(5g_1 + 1)\,(2g_1 - 1)^2$$

since $q \leq 6(2g_1 - 1)$ by Lemma 1.2. Since $g_1 = 1$ or 2, we have

$$36p^2(5g_1 + 1)\,(2g_1 - 1)^2 < B(p, g_1 p),$$

as can be checked easily. Thus we may assume that $u > (5g_1 + 1)qp$. From the equality

$$\frac{2g-2}{uqp} = \frac{2g-2}{n} = \frac{d_1' - 1}{qp} - \frac{1}{e_2}$$

we get $(2g-2)/uqp \geq 1/qpe_2$, which gives $u \leq (2g-2)e_2$. Since $\mu = 0$, we have $\deg \mathfrak{D}_{K/K_1} = 2(p-1)$. This implies that $d_1' = p-1$ and we get

$$\frac{2g-2}{uqp} = \frac{p-2}{qp} - \frac{1}{e_2}$$

$$= \frac{(5g_1+1)(p-2)}{(5g_1+1)qp} - \frac{2g-2}{(2g-2)e_2}$$

$$> \frac{(5g_1+1)(p-2)}{u} - \frac{2g_1p-2}{u}$$

since $u > (5g_1+1)qp$ and $u \leqslant (2g-2)e_2$. Thus we have

$$\frac{2g-2}{uqp} > \frac{(3g_1+1)(p-2) - 4g_1+2}{u} \geqslant \frac{1}{u}$$

since $g_1 = 1$ or 2 and $p \geqslant 3$. This proves $e_1 = qp < 2(g-1)$. Therefore, by (*),

$$n < 24(g-1)^2(2g-1) < B(p, g)$$

since $qp \leqslant 2g-2$ implies $p \leqslant 2g-2$ implies $p \leqslant g+1$, by Lemma 2.4. This completes the proof in the case $g_1 \geqslant 1$.

Case IV(b): $g_1 = 0$. In this case, as in the proof of Theorem 2.1, we have:

(i) K_1/K_0 is a Galois extension of degree q coprime to p and $g_{K_1} = 0$;

(ii) the ramification index of $\mathfrak{p}_1 = \mathfrak{p} \cap K_1$ in K_1/K_0 is q;

(iii) $g_{K_0} = 0$;

(iv) there exists a prime divisor $\mathfrak{q}_1$ of K_1, other than $\mathfrak{p}_1$, which has ramification index q in K_1/K_0;

(v) no prime divisor of K_1 other than $\mathfrak{p}_1$, $\mathfrak{q}_1$ is ramified in K_1/K_0.

Let p^β be the ramification index of $\mathfrak{q}_1$ in K/K_1, $0 \leqslant \beta \leqslant \alpha$. Let $\mathfrak{s} = \mathfrak{p} \cap L$, $\mathfrak{p}_0 = \mathfrak{p} \cap K_0$ and let $\mathfrak{p}_0, \mathfrak{p}_{01}, \ldots, \mathfrak{p}_{0w}$ be all the (distinct) prime divisors of K_0 lying over $\mathfrak{s}$. $w \geqslant 0$. Let $u = [K_0 : L]$. Then

$$u = 1 + \sum_{i=1}^{w} e_{\mathfrak{p}_{0i}|\mathfrak{s}}$$

since $e_{\mathfrak{p}_0|\mathfrak{s}} = 1$. If $w = 0$, then $u = 1$, so that $n = e_1 < B(p, g)$ by Theorem 2.1. Let therefore $w \geqslant 1$. Let $\mathfrak{q}_0 = \mathfrak{q}_1 \cap K_0$. We consider the two cases $\{\mathfrak{p}_{01}, \ldots, \mathfrak{p}_{0w}\} = \{\mathfrak{q}_0\}$ and $\{\mathfrak{p}_{01}, \ldots, \mathfrak{p}_{0w}\} \neq \{\mathfrak{q}_0\}$. First, if $\{\mathfrak{p}_{01}, \ldots, \mathfrak{p}_{0w}\} = \{\mathfrak{q}_0\}$, then $u = 1 + e_{\mathfrak{q}_0|\mathfrak{s}}$. Since $\mathfrak{s}$ is ramified in K/L with ramification index qp^α and $e_{\mathfrak{q}_1|\mathfrak{q}_0} = q$ (by (iv) above), we have $e_{\mathfrak{q}_0|\mathfrak{s}} \leqslant p^\alpha$. Thus

$$u \leqslant 1 + p^\alpha \leqslant \frac{4pg^2}{(p-1)^2} + 1,$$

by Lemma 2.4. Therefore, by Theorem 2.1,

$$n = qp^\alpha u \leqslant \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)\left(\frac{4pg^2}{(p-1)^2} + 1\right) = B(p, g).$$

It now remains finally to consider the case $\{\mathfrak{p}_{01}, \ldots, \mathfrak{p}_{0w}\} \neq \{\mathfrak{q}_0\}$. In this case we have:

Claim. *One of the following two conditions is satisfied:*

(a) $e_1 \leqslant 2pg/(p-1)$ *and* $p-1 \leqslant g$;

(b) $e_1 \leqslant 2g^2/(p-1)$ *and* $p(p-1) \leqslant g$.

Assume the claim for a moment. Then if (a) is satisfied, we have

$$\begin{aligned} n &\leqslant 12e_1(g-1)(2g-1) \qquad \text{(by (*))} \\ &\leqslant 24pg(g-1)(2g-1)/(p-1) \\ &< B(p, g) \qquad \text{since } p-1 \leqslant g, \text{ by (a).} \end{aligned}$$

If (b) is satisfied, then

$$\begin{aligned} n &\leqslant 12e_1(g-1)(2g-1) \qquad \text{(by (*))} \\ &\leqslant 24g^2(g-1)(2g-1)/(p-1) \\ &< B(p, g) \qquad \text{since } p(p-1) \leqslant g, \text{ by (b).} \end{aligned}$$

So we have only to prove the claim.

Proof of the claim. We have $\{\mathfrak{p}_{01}, \ldots, \mathfrak{p}_{0w}\} \neq \{\mathfrak{q}_0\}$, and we may assume, without loss of generality, that $\mathfrak{p}_{01} \neq \mathfrak{q}_0$. Let $K \supset K' \supset K'' \supset K_0$ be as in the proof of Theorem 2.1. (Recall that $g_{K''} = 0, g' = g_{K'} \geqslant 1$ and $[K' : K''] = p$.) Let s be the number of prime divisors of K'' ramified in K'/K''. Note that, since $\mathfrak{p}'' = \mathfrak{p} \cap K''$ is ramified in K'/K'', we have $s \geqslant 1$. Recall that qp^β is the ramification index of $\mathfrak{q}_0$ in K/K_0, $\beta \geqslant 0$. Let s_0 be the number of prime divisors of K_0, other than $\mathfrak{p}_0, \mathfrak{q}_0$, which are ramified in K/K_0, $s_0 \geqslant 0$. With this notation we prove the following five statements:

(1) If $s_0 \geqslant 1$, then $e_1 \leqslant 2g$ and $p-1 \leqslant g$.

(2) If $s_0 = 0$ and $\beta = 0$, then $e_1 \leqslant g-1$ and $p-1 \leqslant g$.

(3) If $s_0 = 0, \beta \geqslant 1$ and $s = 1$, then $e_1 \leqslant 2g^2/(p-1)$ and $p(p-1) \leqslant g$.

(4) If $s_0 = 0, \beta \geqslant 1, s \geqslant 2$ and $\alpha \geqslant 2$, then $e_1 \leqslant 2g^2/(p-1)$ and $p(p-1) \leqslant g$.

(5) If $s_0 = 0, \beta \geqslant 1, s \geqslant 2$ and $\alpha = 1$, then $e_1 \leqslant 2pg/(p-1)$ and $p-1 \leqslant g$.

Note that one of the above five case has necessarily to occur, so that it is enough to prove these five statements.

(1) Let $\mathfrak{r}_0 \neq \mathfrak{p}_0, \mathfrak{q}_0$ be a prime divisor of K_0 ramified in K/K_0. Then, by our observations (ii), (iv) and (v) above, $\mathfrak{r}_0$ is not ramified in K_1/K_0. Therefore, the ramification index of $\mathfrak{r}_0$ in K/K_0 is a power of p, say p^γ, $\gamma \geqslant 1$. Therefore, by Hurwitz' Formula and by Lemma 1.1, we have

$$\frac{2g-2}{qp^\alpha} \geqslant -2 + \frac{qp^\alpha - 1 + p^\alpha - 1}{qp^\alpha} + \frac{qp^\beta - 1 + p^\beta - 1}{qp^\beta} + \frac{2p^\gamma - 2}{p^\gamma},$$

which implies $qp^\alpha \leqslant 2g$ as in Case I(a) of Theorem 2.1. This also gives $p \leqslant 2g$, so that $p \leqslant g + 1$ by Lemma 2.4.

(2) The assumption $s_0 = 0$ and $\mathfrak{p}_{01} \neq \mathfrak{q}_0$ imply that $\mathfrak{p}_{01}$ is not ramified in K/K_0. Therefore, $e_{\mathfrak{p}_{01}|\mathfrak{p}} = qp^\alpha$ which gives $qp^\alpha < u$. Also, $s_0 = 0$ and $\beta = 0$ imply that $\mathfrak{p}_1$ is the only prime divisor of K_1 ramified in K/K_1. Therefore, by Hurwitz' Formula applied to K/K_1, we have

$$\frac{2g-2}{p^\alpha} = -2 + \frac{p^\alpha - 1 + d_1'}{p^\alpha},$$

which gives $d_1' - 1 = p^\alpha + 2g - 2$. Therefore we get

$$\frac{2g-2}{uqp^\alpha} = \frac{2g-2}{n} = \frac{d_1'-1}{qp^\alpha} - \frac{1}{e_2} \qquad (\geqslant 1/qp^\alpha e_2)$$

$$= \frac{p^\alpha + 2g - 2}{qp^\alpha} - \frac{2g-2}{(2g-2)e_2}$$

$$> \frac{p^\alpha + 2g - 2 - (2g-2)}{u},$$

since $qp^\alpha < u$, and $(2g-2)/uqp^\alpha \geqslant 1/qp^\alpha e_2$ implies $u \leqslant (2g-2)e_2$. Thus we have

$$\frac{2g-2}{uqp^\alpha} > \frac{p^\alpha}{u} \geqslant \frac{2}{u},$$

which shows that $qp^\alpha < g-1$. This also implies $p < g-1$.

(3) Let $[K : K'] = p^\delta$, $[K'' : K_1] = p^\epsilon$, $\delta, \epsilon \geqslant 0$. Let $\mathfrak{q}_1$ be as in observation (iv) above. Since $g_{K_1} = 0 = g_{K''}$, it is easy to see by Hurwitz' Formula applied to K''/K_1 that no prime divisor of K_1, other than $\mathfrak{p}_1$, is ramified in K''/K_1. This, together with the assumption that $s = 1$, implies that $\mathfrak{q}_1$ is not ramified in K'/K_1 and therefore it splits into $p^{\epsilon+1}$ prime divisors of K' and each of these $p^{\epsilon+1}$ prime divisors of K' is ramified in K/K' with ramification index p^β. This implies, in particular, that $\delta \geqslant \beta$, and we have, by Hurwitz' Formula applied to K/K' and by Lemma 1.1,

$$\frac{2g-2}{p^\delta} \geqslant 2g' - 2 + \frac{2p^\delta - 2}{p^\delta} + p^{\epsilon+1}\,\frac{2p^\beta - 2}{p^\beta},$$

which gives

$$\frac{2g}{p^\delta} \geqslant 2g' + p^{\epsilon+1}\,\frac{2p^\beta - 2}{p^\beta}.$$

Therefore

$$(*) \qquad g \geqslant (g' + p - 1)p$$

since $\delta \geqslant \beta \geqslant 1$. Next, by Hurwitz' Formula applied to K/K_1, we have

$$\frac{2g-2}{p^\alpha} \geqslant -2 + \frac{2p^\alpha - 2}{p^\alpha} + \frac{2p^\beta - 2}{p^\beta}.$$

Therefore

$$\frac{2g}{p^\alpha} \geqslant \frac{2p^\beta - 2}{p^\beta} \geqslant \frac{2p-2}{p},$$

since $\beta \geqslant 1$. This gives

$$p^\alpha \leqslant \frac{pg}{p-1}.$$

Also, by Lemma 2.4, we have $q \leqslant 2g' + p - 1$. Therefore

$$qp^\alpha \leqslant (2g' + p - 1)\frac{pg}{p-1} < \frac{2g}{p}\frac{pg}{p-1} \qquad \text{(by (*))}$$

$$= \frac{2g^2}{p-1}.$$

Finally, $p^\alpha \leqslant pg/(p-1)$ implies $p^{\alpha-1}(p-1) \leqslant g$ implies $p(p-1) \leqslant g$ since $\alpha - 1 \geqslant \delta \geqslant \beta \geqslant 1$.

(4) Note first that, as in (3), we have $p^\alpha \leqslant pg/(p-1)$. Since $\alpha \geqslant 2$ by assumption, this implies $p(p-1) \leqslant g$. We have now to prove that $qp^\alpha \leqslant 2g^2/(p-1)$. Since $s \geqslant 2$, there exists a prime divisor, say $\mathfrak{r}''$, of K'' such that $\mathfrak{r}'' \neq \mathfrak{p}''$ and $\mathfrak{r}''$ is ramified in K'/K''. The assumption $s_0 = 0$ together with the fact that $\mathfrak{q}_1$ is the only prime divisor of K_1 lying over $\mathfrak{q}_0$ (by our observation (iv) above) implies then that $\mathfrak{r}'' \cap K_1 = \mathfrak{q}_1$. Therefore, this case is precisely Case I(b) of Theorem 2.1. We have proved there that $qp^\alpha \leqslant 2pg$. Since $p(p-1) \leqslant g$, as observed above, we have $2pg \leqslant 2g^2/(p-1)$.

(5) Since $\alpha = 1$, we have $K = K' \supset K'' = K_1$. Since $1 = \alpha \geqslant \beta \geqslant 1$, we have $\beta = 1$. Thus both the prime divisors $\mathfrak{p}_0$ and $\mathfrak{q}_0$ of K_0 have ramification index qp in K/K_0, and thus both are totally ramified in K/K_0. This implies, in view of the assumption $s_0 = 0$, that exactly two prime divisors $\mathfrak{p}_1$ and $\mathfrak{q}_1$ of K_1 are ramified in K/K_1. Since K_1 is rational, we have $K_1 = k(x)$ for some $x \in K_1$. We may choose x such that $\mathfrak{p}_1 = (x)_\infty$ and $\mathfrak{q}_1 = (x)_0$, i.e., $\mathfrak{p}_1$ and $\mathfrak{q}_1$ are respectively the pole divisor and the zero divisor of x in K_1. Since K/K_1 is cyclic of degree p, it is an Artin–Schreier extension, i.e., there exists $y \in K$ such that $K = k(x, y)$ and $y^p - y = f \in K_1$. Let us write $f = x^{-m} f_1$ with $m \in \mathbf{Z}, f_1 \in K_1, f_1(0) \neq 0, \infty$. Then $m > 0$ and we may modify y and f suitably to assume that $f_1 \in k[x]$ and $(m, p) = 1$ (Lemma 1.3). Now, by Lemma 1.1, $G_0/G_1 = \mathrm{Gal}(K_1/K_0)$ is a cyclic group of order q. Let σ be a generator of G_0/G_1. Since $\mathfrak{p}_0$ and $\mathfrak{q}_0$ are totally ramified in K_1/K_0, we have $\sigma(\mathfrak{p}_1) = \mathfrak{p}_1$ and $\sigma(\mathfrak{q}_1) = \mathfrak{q}_1$. Since $\mathfrak{p}_1 = (x)_\infty$ and $\mathfrak{q}_1 = (x)_0$, we get $\sigma(x) = ax$ with $a \in k^*$ a primitive q^{th} root of unity. Since σ extends to an automorphism of K/K_0, there exist, by Lemma 1.3, $h \in K_1$ and $c \in \mathbf{F}_p^*$ such that

$$h^p - h = \sigma(f) - cf = a^{-m} x^{-m} (f_1(ax) - a^m c f_1).$$

From this we get $a^m c = 1$, as in the proof of Case I(b) of Theorem 2.1. Therefore we have

$$(*) \qquad h^p - h = a^{-m} x^{-m} (f_1(ax) - f_1).$$

Let $v = \deg f_1$. *We claim that we can further modify y and f to achieve* $v = 2m$. Suppose this is done. Then it easily follows from the equation (*) that we have $a^{2m} = 1$. (Use the fact that $(m, p) = 1$.) This gives $q \leqslant 2m$. Also, $v = 2m$ implies, by Lemma 1.3, that the exponent of both $\mathfrak{p}$ and $\mathfrak{q}$ in $\mathfrak{D}_{K/K_1}$ is $(m+1)(p-1)$, where $\mathfrak{q}$ is the prime divisor of K lying over $\mathfrak{q}_1$. Therefore, $\deg \mathfrak{D}_{K/K_1} = 2(m+1)(p-1)$ and, by Hurwitz' Formula applied to K/K_1, we get

$$2g - 2 = -2p + 2(m+1)(p-1),$$

so that $g = m(p-1)$. Therefore $p - 1 \leqslant g$ and

$$e_1 = qp \leqslant 2mp = 2pg/(p-1).$$

This proves the statement (5) modulo our claim about the degree of f_1.

In order to prove the claim, we first remark that $\mathfrak{p}_1 \cap L = \mathfrak{q}_1 \cap L$. For we are in the case $r = 2$, i.e., exactly two prime divisors of L are ramified in K/L with ramification indices e_1 and e_2. Since we have assumed $(e_2, p) = 1$ and since p divides the ramification indices in K/L of both $\mathfrak{p}_1 \cap L$ and $\mathfrak{q}_1 \cap L$, we have $\mathfrak{p}_1 \cap L = \mathfrak{q}_1 \cap L$. Therefore, if $\mathfrak{q}$ is the prime divisor of K lying over $\mathfrak{q}_1$, there exists $\tau \in G$ such that $\tau(\mathfrak{p}) = \mathfrak{q}$. Since $\mathfrak{p}$ and $\mathfrak{q}$ are both totally ramified in K/K_0 and since $K_0 = K^{G_0}$, we have $G(\mathfrak{p}) = G_0 = G(\mathfrak{q})$ and $\tau(G_0) = G_0$. It follows that $\tau(G_1) = G_1$. Therefore, $\tau(K_1) = K_1$. Let $\tau_1 = \tau | K_1$. Then $\tau_1(\mathfrak{p}_1) = \mathfrak{q}_1$. Since $\mathfrak{p}_1 = (x)_\infty$ and $\mathfrak{q}_1 = (x)_0$, we have $\tau_1(x) = 1/x$, after replacing x by λx, $\lambda \in k^*$, if necessary. Since $\tau_1 = \tau | K_1$, there exist, by Lemma 1.3, $h \in K_1$ and $c \in \mathbf{F}_p^*$ such that

$$h^p - h = \tau_1(f) - cf = x^m f_1(1/x) - c x^{-m} f_1.$$

It follows from this that $v \geqslant 2m$. For, let v be the discrete valuation of K_1 defined by $\mathfrak{q}_1 = (x)_0$. If $v < 2m$, then

$$v(x^m f_1(1/x)) = m - v > -m = v(c x^{-m} f_1),$$

so that $v(h^p - h) = v(x^m f_1(1/x) - c x^{-m} f_1) = -m$. This shows that $v(h) < 0$ and $-m = pv(h)$, which contradicts the assumption that $(m, p) = 1$. Thus $v \geqslant 2m$. We want $v = 2m$. So suppose $v > 2m$. Then $m - v < -m$ and it follows that $v(h^p - h) = m - v < 0$, so that $v(h) < 0$ and $m - v = pv(h)$. Let $t = -v(h)$. Then $t > 0$ and we have $v = m + tp$. Therefore, letting $f_1 = \lambda_v x^v + \lambda_{v-1} x^{v-1} + \ldots + \lambda_0$, $\lambda_i \in k$, the equation $y^p - y = x^{-m} f_1$ can be written as

$$y^p - y = \lambda_v x^{tp} + x^{-m}(\lambda_{v-1} x^{v-1} + \ldots + \lambda_0)$$

$$= (\lambda_v^{1/p} x^t)^p - \lambda_v^{1/p} x^t + x^{-m}(\lambda_{v-1} x^{v-1} + \ldots + \lambda_0 + \lambda_v^{1/p} x^{t+m}).$$

It follows that changing y to $y - \lambda_v^{1/p} x^t$ decreases v since $t + m < tp + m = v$. Thus we can decrease v till $v = 2m$ is achieved.

This completes the proof of (A). With the proof of (B) in the following theorem, Theorem 3.1 will be completely proved.

Theorem 3.3. *Let K/k be the function field defined by $K = k(x, y)$ with*

(i) $y^p - y = x^{p+1}$, $p \geqslant 3$; *or*

(ii) $y^p - y = x^2$, $p \geqslant 5$.

Let $G = \mathrm{Aut}_k K$ and let g be the genus of K/k. Then

$$|G| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)\left(\frac{4pg^2}{(p-1)^2} + 1\right).$$

(We remark that (ii) is Roquette's example in [6].)

Proof. We assert that there exists an automorphism σ of K/k such that $\sigma(x) \notin k(x)$. For, if K is given by equation (i), then we can define σ by $\sigma(x) = x/y$ and $\sigma(y) = -1/y$. If K is given by (ii), then we define σ by $\sigma(x) = x/y^{(p+1)/2}$ and $\sigma(y) = (y-1)/y$. These are clearly well-defined, and this proves our assertion. The theorem now follows from the following more general:

Theorem 3.3'. (i) *Let $p > 0$ and let K/k be a function field of genus $g \geqslant 2$. Assume that there exists $\mathfrak{p} \in P_K$ such that*

$$|G(\mathfrak{p})| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right).$$

Let $G = \mathrm{Aut}_k K$. Then either $G = G(\mathfrak{p})$ or

$$|G| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)\left(\frac{4pg^2}{(p-1)^2} + 1\right).$$

(ii) *Let $p > 0$ and let K/k be the function field defined by $K = k(x, y)$ with $y^p - y = x^{p^r+1}$, $r \in \mathbf{Z}^+$. If $p = 2$, assume that $r \geqslant 2$, and if $p = 3$, assume that $r \geqslant 1$. Let $g = g_K$ and $G = \mathrm{Aut}_k K$. Then*

$$|G| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)\left(\frac{4pg^2}{(p-1)^2} + 1\right)$$

or

$$|G| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)$$

according as there does or does not exist $\sigma \in G$ such that $\sigma(x) \notin k(x)$.

(iii) *Conversely, let $p > 0$ and let K/k be a function field of genus $g \geqslant 2$ and let $G = \mathrm{Aut}_k K$. If*

$$|G| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)\left(\frac{4pg^2}{(p-1)^2} + 1\right),$$

then K can be defined by $K = k(x, y)$ with $y^p - y = f$, where $f \in k[x]$ is a polynomial of degree $p^r + 1$; there exists a unique prime divisor $\mathfrak{p}$ of K lying over the pole divisor of x in $k(x)$; we have

$$|G(\mathfrak{p})| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right);$$

and there exists $\sigma \in G$ such that $\sigma(x) \notin k(x)$.

Proof. (i) By Theorem 2.2 (iii) (1), we have $2g = p^r(p-1)$ for some $r \in \mathbf{Z}^+$. Let

$$B(p, g) = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right)\left(\frac{4pg^2}{(p-1)^2} + 1\right).$$

By what we have proved in Theorem 3.1, we have $|G| \leqslant B(p, g)$. Therefore we have to show that either $G = G(\mathfrak{p})$ or $|G| \geqslant B(p, g)$. Suppose $G \neq G(\mathfrak{p})$. Let $K_0 = K^{G(\mathfrak{p})}$, $L = K^G$ and $u = [K_0 : L]$. Let $\mathfrak{p}_0 = \mathfrak{p} \cap K_0$ and $\mathfrak{s} = \mathfrak{p} \cap L$. Since $G \neq G(\mathfrak{p})$, we have $u \geqslant 2$. Therefore there exists $\mathfrak{q}_0 \in P_{K_0}$, $\mathfrak{q}_0 \neq \mathfrak{p}_0$, such that $\mathfrak{q}_0 \cap L = \mathfrak{s}$. We claim that $p^{2r+1} \mid e_{\mathfrak{q}_0|\mathfrak{s}}$. For, suppose $p^{2r+1} \nmid e_{\mathfrak{q}_0|\mathfrak{s}}$. Let G_1 be the first ramification group of $\mathfrak{p}$ in K/L and let $K_1 = K^{G_1}$. Since $2g = p^r(p-1)$, we have

$$|G(\mathfrak{p})| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right) = p^{2r+1}(p^r+1)(p-1),$$

and it follows that $|G_1| = p^{2r+1}$. Choose $\mathfrak{q}_1 \in P_{K_1}$ lying over $\mathfrak{q}_0$ and $\mathfrak{q} \in P_K$ lying over $\mathfrak{q}_1$. Since

$$e_{\mathfrak{q}|\mathfrak{s}} = e_{\mathfrak{p}|\mathfrak{s}} = |G(\mathfrak{p})| = p^{2r+1}(p^r+1)(p-1)$$

and since $(e_{\mathfrak{q}_1|\mathfrak{q}_0}, p) = 1$, our assumption $p^{2r+1} \mid e_{\mathfrak{q}_0|\mathfrak{s}}$ implies that $e_{\mathfrak{q}|\mathfrak{q}_1} = p^\beta$ with $\beta \geqslant 1$. Thus the prime divisors $\mathfrak{p}_1 = \mathfrak{p} \cap K_1$ and $\mathfrak{q}_1$ of K_1 are ramified in K/K_1 with ramification indices p^{2r+1} and p^β, respectively. Therefore, by Hurwitz' Formula applied to K/K_1 and by Lemma 1.1, we have

$$\frac{2g-2}{p^{2r+1}} \geqslant 2g_{K_1} - 2 + \frac{2p^{2r+1}-2}{p^{2r+1}} + \frac{2p^\beta - 2}{p^\beta} \geqslant \frac{-2}{p^{2r+1}} + \frac{2p-2}{p}$$

since $\beta \geqslant 1$. This gives $2g \geqslant 2p^{2r}(p-1)$, which is a contradiction since $2g = p^r(p-1)$. This proves that $p^{2r+1} \mid e_{\mathfrak{q}_0|\mathfrak{s}}$. Therefore

$$u \geqslant e_{\mathfrak{p}_0|\mathfrak{s}} + e_{\mathfrak{q}_0|\mathfrak{s}} \geqslant 1 + p^{2r+1} = 1 + 4pg^2/(p-1)^2,$$

and it follows that $|G| = u\,|G(\mathfrak{p})| \geqslant B(p, g)$. This proves (i).

(ii) Let $\mathfrak{p}$ be a prime divisor of K lying over the pole divisor of x in $k(x)$. Then, by Theorem 2.2 (ii), we have

$$|G(\mathfrak{p})| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right).$$

By Theorem 2.2 (i), we also have $2g = p^r(p-1)$. Therefore our assumptions on p and r imply that $g \geqslant 2$. Finally, we note from the proof of Theorem 2.2 (ii) that $G(\mathfrak{p}) = \{\sigma \in G : \sigma(x) \in k(x)\}$. The assertion now follows from (i) above.

(iii) We note from the proof of Theorem 3.1 that we have obtained the strict inequality $|G| < B(p, g)$, except when $\{\mathfrak{p}_{01}, \ldots, \mathfrak{p}_{0w}\} = \{\mathfrak{q}_0\}$ in Case IV(b). Moreover, if the equality occurs in that case, then with $\mathfrak{p}$ as in Case IV(b) of Theorem 3.1, we necessarily have

$$|G(\mathfrak{p})| = \frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right).$$

Therefore, by Theorem 2.2 (iii), there exist $x, y \in K$ such that
(1) $K = k(x, y)$ with $y^p - y = f$, where $f \in k[x]$ is of degree p^r+1 for some $r \in \mathbf{Z}^+$;
(2) $G(\mathfrak{p}) \supset \{\sigma \in G \mid \sigma(x) \in k(x)\}$.
Since $|G| = B(p, g)$, we have $G \neq G(\mathfrak{p})$. Therefore, in view of (2), there exists $\sigma \in G$ such that $\sigma(x) \notin k(x)$.

Corollary 3.4. *If $p = 2$, then we always have the strict inequality $|G| < B(p, g)$.*

Proof. Suppose K is defined by $y^2 - y = f \in k[x]$. Then K is a hyperelliptic field, so that $k(x)$ is the unique rational subfield of K of index 2. Therefore, every automorphism of K/k carries $k(x)$ into $k(x)$. The corollary now follows from Theorem 3.3′ (iii).

Added in proof. After this work was done, the author learnt that the same problem has been treated independently by Stichtenoth and that he has obtained good upper bounds for the group of automorphisms of a function field of genus at least two.

References

[1] C. Chevalley, Introduction to the Theory of Algebraic Functions of one Variable (Am. Math. Soc., Providence, R.I., 1951).
[2] H. Hasse, Theorie der relative zyklischen algebraischen Funktionenkörper, Crelle 172 (1934) 37–54.
[3] H. Hasse, Zahlentheorie, 2nd ed. (Akademie-Verlag, Berlin, 1963).
[4] A. Hurwitz, Über algebraische Gebilde mit eindeutigen Transformationen in sich, Math. Ann. 41 (1893) 403–442.
[5] K. Iwasawa and T. Tamagawa, On the group of automorphisms of a function field, J. Math. Soc. Japan 3 (151) 137–147; 4 (1952) 100–101, 203–204.
[6] P. Roquette, Abschätzung der Automorphismenanzahl von Funktionenkörpern, Math. Z. 117 (1970) 157–163.
[7] H.L. Schmid, Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik, Crelle 179 (1938) 5–15.
[8] J.-P. Serre, Corps Locaux (Hermann, Paris, 1962).